REMARKS

The Office Action dated November 27, 2007, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 29-38, 43-44, and 54-60 are pending in the application. Claims 29-38, 43-44, and 54-60 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 45 is canceled. No new matter is added. Applicant submits the pending claims for consideration in view of the following.

Claims 29-38, 43-45, and 54-60 were rejected under 35 U.S.C. §103(a) as being unpatentable over Handley et al. ("Network Working Group," March 1999 – hereinafter Handley) in view of Nuutinen (US 6,865,681 – hereinafter Nuutinen) and further in view of Hardjono (US 6,425,004 – hereinafter Hardjono). This rejection is traversed as follows.

Claim 29, upon which claims 30-45 depend, is generally directed to an apparatus that includes a transmitter configured to send, during a subscriber equipment terminated call, a session invitation message to a subscriber equipment. The session invitation message includes authentication information. The apparatus also includes a determiner configured to determine whether a verification of the authentication is required. The apparatus also includes a processor configured to, if the verification is not required, forward a scheduled result to a network control element by including the scheduled result into the session invitation message. The processor is also configured to, if the network control element has to perform the verification, receive the scheduled result from another

network control element, wherein the scheduled result is included in the session invitation message, extract the scheduled result from the session invitation message, forward the session invitation message without the scheduled result to the subscriber equipment, verify an authentication result with the scheduled result, and repeat the verification for a predetermined number of times using different authentication information.

Claim 54, upon which claims 55-58 depend, is generally directed to a method that includes sending, during a subscriber equipment terminated call, a session invitation message from a network control element to the subscriber equipment. The session invitation message includes authentication information. The method also includes determining, by the network control element, whether the network control element has to perform a verification of the authentication or not. In case the network control element does not have to perform the verification, the method continues by forwarding a scheduled result to a second network control element by including the scheduled result into the session invitation message. In case the network control element has to perform the verification, the method continues by receiving the scheduled result from another network control element, wherein the scheduled result is included in the session invitation message, extracting the scheduled result from the session invitation message, forwarding the session invitation message without the scheduled result to the subscriber equipment, verifying an authentication result with a scheduled result, and repeat the verification for a predetermined number of times using different authentication information.

Claim 59 is generally directed to a computer program embodied on a computer-readable medium. The computer program includes computer code for causing a processor to perform operations that include sending a session invitation message from a network control element to the subscriber equipment. The session invitation message including authentication information. The computer program also includes operations for determining, by the network control element, whether the network control element has to perform a verification of the authentication or not. In case the network control element does not have to perform the verification, the operations continue by forwarding a scheduled result to a second network control element by including the scheduled result into the session invitation message. In case the network control element has to perform the verification, the operations continue by receiving the scheduled result from another network control element, wherein the scheduled result is included in the session invitation message, extracting the scheduled result from the session invitation message, forwarding the session invitation message without the scheduled result to the subscriber equipment, and verifying an authentication result with a scheduled result, and repeat the verification for a predetermined number of times using different authentication information.

Claim 60 is generally directed to an apparatus that includes a sending means for sending, during a subscriber equipment terminated call, a session invitation message to the subscriber equipment. The session invitation message including authentication information. The apparatus also includes a determining means for determining whether a verification of the authentication is required and a transceiver means for forwarding a

scheduled result to a second control network by including the scheduled result into the session invitation message, if the verification is not required. If the verification is required, the transceiver means is configured for receiving the scheduled result from another network control element, where the scheduled result is included in the session invitation message. Also, the apparatus includes an extracting means for extracting the scheduled result from the session invitation message and to forward the session invitation message without the scheduled result to the subscriber equipment, a verification means for verifying an authentication result with a scheduled result, and repeat the verification for a predetermined number of times using different authentication information.

Each of the foregoing claims recites limitations that are not disclosed or suggested by combination of Handley, Nuutinen, and Hardjono.

Handley is directed to SIP protocol. In Hadley, the INVITE message indicates that a user or service is being invited to participate in a session. The message contains a description of the session to which the callee is being invited. A user that wishes to authenticate itself with a server may include an authorization request-header field with the request. The authorization field value consists of credentials containing the authentication information of the user agent. Handley further describes a Proxy-Authorization request-header field that allows the client to identify itself to a proxy which requires authentication. Handley further states that "unlike Authorization, the Proxy-Authorization header field applies only to the next outbound proxy that demanded authentication using the Proxy-Authenticate field."

Nuutinen is directed to a secure voice over internet protocol (VoIP) terminal that includes a modular security manager for use in conjunction with a protocol stack. In Nuutinen a security manager includes a plurality of interfaces to the stack. The interfaces may include a security stack interface (SSA) between an SIP manager of an SIP stack and the security manager, a security terminal interface (SST) between a telephony application and the security manager, a security media interface (SSM) between the security manager and a media controller, and a security manager application interface (SMA) between the security manager and a security application (PGP) outside the stack.

Hardjono is directed to a technique for detecting and locating a misbehaving router. The technique divides the network domain into multiple sectors and uses a two-level authentication scheme to allow a receiving device to authenticate that a particular packet originated in a particular sector. Upon receiving the packet, a receiving device authenticates the packet by computing a sector verification tag and comparing the sector verification tag to the sector tag in the packet.

According to Hardjono, if the sector verification tag does not match the sector tag in the packet, then the receiving device drops the packet. If the sector verification tag matches the sector tag in the packet, but the packet includes invalid data, then the receiving device forwards the packet to a secure and trusted authority in the receiving sector. The secure and trusted authority in the receiving sector forwards the packet to other secure and trust authorities in other sectors. Each secure and trusted authority that receives the packet is able to determine whether any device in its sector is the originating

device for the packet by computing device verification tags for each device in the sector and comparing the device verification tags to the device tag in the packet.

However, a combination of Handley, Hardjono, and Nuutinen fails to disclose or suggest, at least, "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

The Office Action takes the position that Handley discloses the "repeating" of claim 54 at pages 114-117. However, a review of these passages demonstrates that Hadley does not disclose "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

For example, page 114 of Handley generally presents proxy-authentication where the client, instead of the proxy, adds the proxy authorization header containing credentials for the proxy which has asked for the authentication. Page 114 of Handley also generally presents a PGP authentication scheme where a server may ascertain the origin of a request based on an existing public key and a private key of the client. Accordingly, page 114 of Handley fails to disclose or suggest "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

Additionally, page 115 of Handley discloses the www-authenticate response header. On this page, Handley discloses the meanings of certain parameters corresponding to a www-authenticate response header. These parameters include a "realm," a "PGP-algorithm," a "PGP-version," and a "nonce." Handley discloses that the realm may include the name of the host. The PGP-algorithm may include an indication

of the PGP message integrity check used to produce a signature. The PGP-version indicates the version of the PGP that the client must use. The nonce indicates the server-specified data string which should be uniquely generated each time a 401 response is made. Handley discloses that the nonce is used to prevent replay attacks and may include a time stamp, but that reply attacks are of little concern such that the server need not keep a nonce record. Accordingly, page 115 of Handley fails to disclose or suggest the "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

Furthermore, page 116 of Handley generally discloses an authorization heading. On this page, Handley discloses that a client increments a CSeq header before each request is retried. Page 116 also discloses other conditions and parameters regarding the authorization heading. As such, page 116 of Handley fails to disclose or suggest "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

Further still, page 117 of Handley generally discloses additional characteristics of an authorization header. On page 117, Handley provides some advantages and draw backs to not generating nonces, using ASCII-armored and PGP signature mechanisms. Page 117 also provides that receivers of signed SIP messages should discard any end-to-end header fields above the authorization header, as they may have been produced with a malicious design. However, page 117 fails to disclose or suggest "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

In light of the above, Handley fails to disclose or suggest, at least, "repeating the verification for a predetermined number of times, wherein different authentication information are used," as recited in claim 54.

Neither Hardjono nor Nuutinen cure the deficiencies of Handley, as noted above. Nuutinen discloses a secure voice over internet protocol (VoIP) terminal that includes a modular security manager for use in conjunction with a protocol stack. Nuutinen discloses a security manager that includes a plurality of interfaces that act as an interface between an SIP manager and a security manager. However, Nuutinen fails to disclose the "repeating" as disclosed in claim 54.

Hardjono is silent with regards to verifying an authentication result with a scheduled result. As discussed above, Hardjono is directed to a technique for detecting and locating a misbehaving router. Thus, repeating a verification of an authentication as recited in claim 54 is not executed in Hardjono.

Therefore, the combination of Handley, Nuutinen, and Hardjono fails to disclose or suggest, "repeating the verification for a predetermined number of times, wherein different authentication information are used." As such, Applicant respectfully requests that this rejection be withdrawn.

Furthermore, Applicant respectfully asserts that the Office Action has failed to presented a *prima facie* case for obviousness. To justify the combination of Handley, Nuutinen, and Hardjono, the Office Action presents the general interest of "efficient transmission." Applicant very respectfully asserts that this justification is so broad that it could provide a rational basis for combining any references that might disclose a feature

that is arguably comparable to a limitation recited in the pending claims. To this issue, MPEP § 2141 states that, "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious." Accordingly, Applicant respectfully submits that the reasoning presented in the Office Action for combining the references sighted is insufficient to support a §103(a) rejection.

Further still, one skilled in the relevant art would not be motivated to combine Handley with Hardjono, as Handley is directed to inviting a user or service to a call session, and Hardjono is directed to detecting misbehaving routers. Indeed, given the highly specialized fields of these references (i.e., SIP protocol INVITE messages and router performance diagnosis in an already established network), a person of ordinary skill in the art would not be motivated to combine Handley with Hardjono. Accordingly, Applicant respectfully asserts that the combination suggested in the Office Action is improperly based upon hindsight bias.

In light of the foregoing, Applicant respectfully requests that the §103(a) rejection of claim 54 be withdrawn. Similarly, Applicant respectfully requests that the §103(a) rejection to claims 29, 59, and 60 be withdrawn as these claim recite similar limitations, though each claim has its own scope. Furthermore, Applicant respectfully requests that the §103(a) rejection of claims 30-38, 43-44, and 55-58 be withdrawn for at least their dependency from claims 29 and 54.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

The foregoing comments made with respect to the positions presented in the Office Action are not be to construed as acquiescence with other positions presented in the Office Action that have not been explicitly contested. Accordingly, the above arguments for patentability of a claim should not be construed as implying that there are not other valid reasons for patentability of the claim or other claims. Additionally, the Applicant does not acquiesce that the cited art anticipates or renders obvious any of the claims as previously presented, and reserve the right to pursue any of the previously presented claims in a subsequent application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Brad Y. Chin
Registration No. 52,738

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

JTO/BYC/jf